nbrss
NATIONAL INSTITUTES OF HEALTH
BUSINESS & RESEARCH SUPPORT SYSTEM

NBS General Users Security Guidelines

July 2002

Security Duties of General Users

As an employee who works with the NBS or NBS related information on a daily basis, you are one of the best advocates and the first line of defense in security. Your vigilance in maintaining security practices is one of the strongest ways to keep the NBS safe. Therefore, NBS users have certain responsibilities associated with security. The following section describes your security responsibilities. With your help, we can keep the NBS and its data secure.

As part of your introduction to NIH and its systems, you should have taken the online computer security-training course. The main topics of the NIH Computer Security Awareness Training course are: NIH IT Security Program, Using IT Resources, Information Management, Local & Remote Access, Internet Safety, Physical Security & Back-Ups, and PC Basics, and References and Information. Completion of this course is required of all employees before they use the NBS. If you have not yet taken this short course, please go to http://irm.cit.nih.gov/sectrain/ after reading the security section and complete the course.

The online course provides a general NIH perspective on security. The following are additional requirements for NBS security maintenance:

- The current password requirements that NBS users will adhere to are:
    - Passwords must be greater than six characters in length.
    - Passwords will use mixed-case alphabetic characters.
    - Passwords will contain non-alphabetic characters, e.g., digits or punctuation.
    - Passwords will be set to expire after 90 days of use at which time the user will be forced to change passwords.
    - New passwords must be different from previous ones.
    - Refer to the NIH Guidance for Selecting Good Passwords located at: http://irm.cit.nih.gov/security/pwd_guidelines.html.

- Label NBS electronic media and documents to indicate the level of sensitivity. The following wording is suggested for labeling storage media and documents containing sensitive material: "Contains sensitive information – Knowing or willful disclosure of sensitive information can result in criminal penalties associated with the Privacy Act, Computer Security Act, and other Federal laws that apply."

- Sensitive NBS information must not be left unattended, even temporarily. Sensitive data must remain in the employee's physical control at all times. Sensitive material should be kept in a secure safe or a locked cabinet and be returned to a secure location each evening or during breaks greater than 30 minutes.

- Large volume output and output that has been labeled "PRIVATE" are considered a special handling category. Centralized printed NBS output at the NIH Computer Center will either be placed in assigned combination lock boxes or in "special handling" boxes. The lock boxes are accessible by only those users who have been given the combination by their account sponsor. Special handling output is distributed at the Output Distribution services counter in the NIH Computer Center. Before such output is released, the user must request it by job name and provide personal identification. "PRIVATE" output must be signed for by the user or by a designated representative.

- Sensitive information being hand-carried to another location must be kept with the individual and protected from unauthorized disclosure.

- Use of personal equipment or software at the workplace requires supervisor approval to prevent accusations of attempted theft when the item is removed at a later date.

- If a workstation must be located in a public area, users are required to log-off the system when it is not in use, or to lock the workstation. Users may also want to consider the use of computer privacy screens.

- CIT-purchased software must be used in accordance with contract agreements and copyright law. Commercial PC software that is purchased by CIT is authorized for CIT use only. Making copies of CIT-purchased software for personal use is prohibited. Employees are prohibited from performing unauthorized modifications of CIT-licensed software.

- Verify that software and systems are checked for computer viruses periodically, and that safe computing procedures are followed.

- In the event of a security episode, such as a virus that is affecting the entire office, user support is available at NIH by calling your local IC help desk, ISSO, or TASC (301-594-6248.

The Center for Information Technology also offers additional security training. If you are interested, their web page located at http://irm.cit.nih.gov/security/sec_train.html, goes into more detail of their opportunities. In addition, the CIT Training Center, located at http://training.cit.nih.gov/, offers a wide variety of computer courses, include security topics.

Supervisors

In addition to the responsibilities of general users, supervisors have some additional duties when it comes to security. The following section reviews the enforcement and regulatory obligations of supervisors:

- Supervisors are responsible for monitoring employee activities to ensure strict compliance with all legal requirements concerning the use of proprietary software, e.g., respecting copyrights and obtaining site licenses.
- Ensure their employees (both government and contractor) are knowledgeable of and observe all of the security requirements for office automation equipment, facilities, and their data.
- Ensure their employees receive appropriate, periodic security training.
- Ensure only authorized software runs on government computing systems.